TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	10/749,649
Filing Date	December 30, 2003
First Named Inventor	Ju-Han Kim
Art Unit	
Examiner Name	
Total Number of Pages in This Submission: 6	Attorney Docket Number: 51876P550

ENCLOSURES *(check all that apply)*

- [X] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
  - [ ] PTO/SB/08
- [X] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Basic Filing Fee
  - [ ] Declaration/POA
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below):*

Request for Priority; return postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Eric S. Hyman, Reg. No. 30,139 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	2/23/04

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	Melissa Stead		
Signature	Melissa Stead	Date	2-23-04

Based on PTO/SB/21 (02-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2004

Effective 01/01/2004. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($)

Complete if Known	
Application Number	10/749,649
Filing Date	December 30, 2003
First Named Inventor	Ju-Han Kim
Examiner Name	
Art Unit	
Attorney Docket No.	51876P550

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

		Extra Claims		Fee from below		Fee Paid
Total Claims		- 20** =		X	=	
Independent Claims		- 3 =		X	=	
Multiple Dependent					=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple Dependent claim, if not paid
1204	86	2204	43	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920 *	1804	920 *	Requesting publication of SIR prior to Examiner action	
1805	1,840 *	1805	1,840 *	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	1,210	2255	605	Extension for reply within fifth month	
1404	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($)

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Eric S. Hyman	Registration No. (Attorney/Agent)	30,139	Telephone	(310) 207-3800
Signature				Date	2/23/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

DOCKET NO.: 51876P550

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

JU-HAN KIM, ET AL.

Application No.: 10/749,649

Filed: December 30, 2003

For: **INTEGRATED SECURITY INFORMATION MANAGEMENT SYSTEM AND METHOD**

Art Group:

Examiner:

Commissioner for Patents
P.O, Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Applicant respectfully requests a convention priority for the above-captioned application, namely:

COUNTRY	APPLICATION NUMBER	DATE OF FILING
Korea	2003-87371	3 December 2003

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 2/23/04

Eric S. Hyman, Reg. No. 30,139

12400 Wilshire Boulevard, 7th Floor
Los Angeles, CA 90025
Telephone: (310) 207-3800

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Melissa Stead 2-23-04

Melissa Stead ***Date***

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0087371
Application Number

출 원 년 월 일 : 2003년 12월 03일
Date of Application DEC 03, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Inst

2003 년 12 월 17 일

특 허 청
COMMISSIONER

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

【서지사항】

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0001
【제출일자】 2003.12.03
【발명의 명칭】 보안 정보 통합 관리 시스템 및 그 방법
【발명의 영문명칭】 Integrated Security Information Management System and Its Method

【출원인】
【명칭】 한국전자통신연구원
【출원인코드】 3-1998-007763-8

【대리인】
【명칭】 특허법인 신성
【대리인코드】 9-2000-100004-8
【지정된변리사】 변리사 정지원, 변리사 원석희, 변리사 박해천
【포괄위임등록번호】 2000-051975-8

【발명자】
【성명의 국문표기】 김주한
【성명의 영문표기】 KIM,Ju Han
【주민등록번호】 720424-1408610
【우편번호】 301-211
【주소】 대전광역시 중구 산성동 136-5
【국적】 KR

【발명자】
【성명의 국문표기】 문기영
【성명의 영문표기】 MOON,Ki Young
【주민등록번호】 631014-1797829
【우편번호】 302-280
【주소】 대전광역시 서구 월평동 누리아파트 101-1203
【국적】 KR

【발명자】
【성명의 국문표기】 손승원
【성명의 영문표기】 SOHN,Sung Won

【주민등록번호】 571225-1674514
【우편번호】 305-390
【주소】 대전광역시 유성구 전민동 엑스포아파트 208-902
【국적】 KR
【발명자】
【성명의 국문표기】 박치항
【성명의 영문표기】 PARK,Chee Hang
【주민등록번호】 470112-1069516
【우편번호】 305-333
【주소】 대전광역시 유성구 어은동 한빛아파트 131-1002
【국적】 KR
【심사청구】 청구
【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
특허법인 신성 (인)
【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	21	면	21,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	10	항	429,000 원

【합계】 479,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 239,500 원
【기술이전】
【기술양도】 희망
【실시권 허여】 희망
【기술지도】 희망
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

1. 청구범위에 기재된 발명이 속하는 기술분야

본 발명은, 보안 정보 통합 관리 시스템 및 그 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 다양한 보안 정보들을 XML(Extensible Markup Language) 기반의 국제 표준에 따라 통합적으로 관리하여 보안 정보의 호환성 및 이동성을 높이기 위한, 보안 정보 통합 관리 시스템 및 그 방법을 제공하는데 그 목적이 있음.

3. 발명의 해결 방법의 요지

본 발명은, 보안 정보 통합 관리 시스템에 있어서, 외부의 보안 정보 통합 관리 클라이언트와 XML(Extensible Markup Language)을 기반으로 인터페이스하고, 사용자를 인증하며, 상기 보안 정보 통합 관리 클라이언트로부터의 요청을 해석한 후 요청의 종류에 따라 접근제어 수단 또는 인증 수단 또는 외부의 공개키 기반 구조 인증 서버로 처리를 요청하기 위한 XML 키 관리 수단; 상기 XML 키 관리 수단으로부터의 공유 보안 정보 처리 요청에 따라 사용자 인증 기능, 제한공유 데이터 저장 수단에 대한 접근 권한 정책 생성 기능, 접근 권한 정책에 따른 접근 권한 확인 기능, 접근이 허용된 사용자에게 공유 보안 정보 제공 기능, 보안 정보 위치 정보 제공 기능, 공유 보안 정보의 등록/삭제/갱신 기능, 공유 보안 정보에 대한 공유 설정/해제 기능, 및 XML 전자서명/검증/암호화/복호화/통신 보안 기능을 제공하기 위한 상기 접근제어 수단; 상기 XML 키 관리 수단으로부터의 비공유 보안 정보 처리 요청에 따라 사용자 인증 기능, 본인 인증 기능, 접근이 허용된 사용자(본인)에게 비공유 보안 정보 제공 기능, 보안 정보

위치 제공 기능, 비공유 보안 정보의 등록/수정/삭제 기능, 및 XML 전자서명/검증/암호화/복호화 통신 보안 기능을 제공하기 위한 상기 인증 수단; 상기 접근제어 수단의 제어에 따라 제한된 대상에게 공유되는 보안 정보를 저장하고 관리하기 위한 상기 제한공유 데이터 저장 수단; 및 상기 인증 수단의 제어에 따라 공유되어서는 안되는 보안 정보를 저장하고 관리하기 위한 비공유 데이터 저장 수단을 포함함.

4. 발명의 중요한 용도

본 발명은 전자상거래, 전자문서거래, 통신, 사이트 접속 및 문서 저장 등의 모든 온라인 분야 등에 이용됨.

【대표도】

도 3

【색인어】

보안 정보 통합 관리, 보안 정보 공유, 공개키 기반 구조(PKI), XML, XML 키 관리 스펙(XKMS)

【명세서】

【발명의 명칭】

보안 정보 통합 관리 시스템 및 그 방법{Integrated Security Information Management System and Its Method}

【도면의 간단한 설명】

도 1은 본 발명에 따른 보안 정보 통합 관리 시스템의 일실시예 구성도.

도 2는 본 발명에 따른 제한공유 데이터 저장소에 대한 일실시예 구조도.

도 3은 본 발명에 따른 비공유 데이터 저장소에 대한 대한 일실시예 구조도.

도 4는 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 등록 과정에 대한 일실시예 흐름도.

도 5는 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 공유 설정/해제 과정에 대한 일실시예 흐름도.

도 6은 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 공유 과정에 대한 일실시예 흐름도.

도 7은 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 갱신 과정에 대한 일실시예 흐름도.

* 도면의 주요 부분에 대한 부호 설명

11 : 확장 XKMS 클라이언트 12 : PKI 인증 서버

13 : 보안 정보 통합 관리 시스템 131 : 확장 XKMS 서버

132 : 접근제어 서버 133 : 인증 서버

134 : 제한공유 데이터 저장소 135 : 비공유 데이터 저장소

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은, 보안 정보 통합 관리 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 다양한 보안 정보들을 XML(Extensible Markup Language) 기반의 국제 표준에 따라 통합적으로 관리하여 보안 정보의 호환성 및 이동성을 높이기 위한, 보안 정보 통합 관리 시스템 및 그 방법에 관한 것이다.

<14> 오늘날 정보통신 기술의 발달로 인하여 전세계적으로 개방형 통신망인 인터넷을 활용한 전자상거래, 전자문서거래, 통신 등의 서비스가 다양한 분야에서 급속하게 확산되고 있다. 이때, 전자상거래란 기업이나 소비자가 정보통신망을 활용하여 행하는 광고, 마케팅, 상품 및 서비스의 교환 등의 모든 경제활동은 물론 이와 관련된 정보의 교환까지도 포괄하는 것으로 정의할 수 있다.

<15> 그런데, 이와 같이 인터넷을 활용한 전자상거래, 전자문서거래 등에서는 모든 정보와 자료가 전자적인 방법으로 교환되기 때문에 기존의 종이서류에 의한 정보교환방법이나 폐쇄형 전자문서교환에 의한 정보교환방법에서는 필요치 않았던 보안이나 인증에 대한 문제점들이 발생

할 수 있다. 즉, 정보교환 당사자간의 신원확인, 교환된 정보의 변조 여부와 관련된 무결성, 당사자 간에 거래 사실 부인 방지 및 교환된 정보의 증거성 확보 등의 문제점이 제기된다.

<16> 이러한 문제점들로 인한 분쟁을 예방하기 위하여 전자상거래, 전자문서거래 등의 모든 단계에서는 보안 기술을 활용하고 이를 관리하는 인증기관이 개입하고 있으며, 대표적인 보안 기술로는 공개키 기반 구조(PKI), 전자서명(Digital Signature), 생체인식 등이 있다.

<17> 먼저, 공개키 기반 구조(Public Key Instructure)는 인터넷과 같은 개방형 또는 분산형 정보통신망 환경에서 사용자 간에 주고받는 정보의 변경 여부를 확인하는 무결성, 사용자의 신분확인을 위한 인증, 사후 자신의 행위에 대한 부인방지 등에 필요한 공개키 암호방식을 이용하는 보안서비스를 효과적으로 이용할 수 있도록 해주는 다수의 인증 기관이 계층적으로 연결된 인증 메커니즘이라 할 수 있다. 즉, 공개키 기반 구조는 무결성, 인증, 부인방지 등의 보안 서비스 제공을 위한 인증서의 생성, 처리, 폐지 등의 과정과 전자서명 생성과 확인에 필요한 비밀키, 공개키 등의 각종 키를 관리하는 하드웨어, 소프트웨어, 정책들의 집합으로 볼 수 있다.

<18> 국내의 공개키 기반 구조(PKI : Public Key Instructure)의 구축과 운영에 관한 기본정책 결정은 정부측의 정보보호분과위원회와 정보통신부가 담당하고 있으며, 한국정보보호센터가 최상위인증기관(Root CA)으로서 공인인증기관(CA)에 대한 인증서 발급 및 공인인증관리를 한다. 공인인증기관(CA)은 가입자에 대한 인증서 발급 등의 인증 업무를 수행하는데, 필요에 따라 등록기관(RA)이 가입자 신원확인 및 등록업무를 대행할 수 있도록 되어 있다. 공개키 기반의 보안 서비스는 2000년 10월 전자서명법 공표와 함께 인터넷 뱅킹을 필두로 현재 급속도로 보급되고 있는 서비스이다.

<19> 그런데, 공개키 기반 구조(PKI) 기술은 다른 종류의 보안 정보까지 관리하지는 않으며, 여러 개의 인증서 및 개인키 등은 다른 관리 도구를 사용하여 개별적으로 관리하여야 한다.

<20> 다른 보안 기술로서, 종래의 인감 혹은 사인(Sign)과 같이 개인의 고유성을 주장하고 인정받기 위하여 전자문서에 서명하는 전자서명(Digital Signature) 기술이 있다.

<21> 전자서명(Digital Signature) 기술은 위조불가(Unforgeable), 서명자 인증(Authentication), 부인방지(Non-Requdiation), 변경불가(Unalterable), 재사용 불가(Not Reusable) 등의 특징을 가지고 있으며, 공개키 기반 구조(PKI) 방식을 사용하는 직접서명 방식과 신뢰할 수 있는 제3자(TTP : Trusted Third Party)를 통해 서명을 생성하고 검증하는 중재자를 통한 서명 방식으로 구분할 수 있다. 특히, 공개키 기반 구조(PKI) 방식을 사용하는 직접서명 방식은 사용자들끼리 공동의 비밀키를 소유하고 있어야 하기 때문에 키 분배라는 복잡한 절차가 필요하게 되는데, 일반 사용자들은 복잡한 키 분배 문제를 해결할 수 없기 때문에, 공신력있는 인증기관(CA : Certificate Authority)에서 키를 관리하고 신원을 보장하는 여러가지 행위를 서비스한다.

<22> 그런데, 이와 같은 공개키 기반 구조(PKI) 방식을 사용하는 보안 기술들은 아직 일정한 표준이 존재하지 않기 때문에, 키를 관리하는 방법이 제각각이고 서로 호환이 안되어 여러 인증서를 가지고 있어야하는 경우가 비일비재하였다. 또한, 같은 종류의 보안 정보라 하더라도 관리 도구에서 요구하는 형태가 모두 다르므로 각 관리도구에 맞게 보안 정보를 재설정해야 하며, 보안 정보의 사용성에도 한계가 있는 문제점이 있었다. 이와 같은 문제점을 해결하기 위하여 개발된 것이 XML 키 관리 스펙(XKMS : XML Key Management Specification)이다.

<23> XML 키 관리 스펙(XKMS)은 기존의 공개키 기반 기술(PKI)과 공개키 인증서, 그리고 XML(eXtensible Markup Language) 애플리케이션의 통합이 용이하도록, 다양하고 복잡한 기능의

전자거래 애플리케이션에서 전자문서의 서명을 검증하거나 암호화하는 공개키를 관리하는 프로토콜을 정의하고 있다.

<24> XML 키 관리 스펙(XKMS)은 XML 키 정보 서비스 스펙(X-KISS : XML Key Information Service Specification)과 XML 키 등록 서비스 스펙(X-KRSS : XML Key Registration Service Specification)의 두 영역으로 구성되어 있다. XML 키 정보 서비스 스펙(X-KISS)은 공개키 위치와 식별자 정보, 및 공개키 연결 기능을 지원하는 프로토콜이며, XML 키 등록 서비스 스펙(X-KRSS)은 키 쌍 소유자에 의한 키 쌍의 등록을 지원하는 프로토콜로서, 각 서비스는 간단한 요청 및 응답으로 구성된다.

<25> 한편, XML 키 관리 스펙(XKMS)은 공개키 기반 기술(PKI)에 이용되는 보안 정보를 XML 기반의 국제 표준에 따라 관리함으로써, 관리 도구들 사이에서 사용되는 보안 정보의 호환성 문제를 해결할 수 있지만, 그 이외의 보안 정보(예를 들어, 인터넷 서비스 등에서 가장 간단하게 널리 사용되는 패스워드(패스프레이즈) 정보, 웹서비스의 보안 토큰, 생체 정보 등을 보안 수준에 따라 통합적으로 관리할 수는 없는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<26> 본 발명은, 상기와 같은 문제점을 해결하기 위하여 제안된 것으로, 다양한 보안 정보들을 XML 기반의 국제 표준에 따라 통합적으로 관리하여 보안 정보의 호환성 및 이동성을 높이기 위한, 보안 정보 통합 관리 시스템 및 그 방법을 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<27> 상기의 목적을 달성하기 위한 본 발명은, 보안 정보 통합 관리 시스템에 있어서, 외부의 보안 정보 통합 관리 클라이언트와 XML(Extensible Markup Language)을 기반으로 인터페이스하고, 사용자를 인증하며, 상기 보안 정보 통합 관리 클라이언트로부터의 요청을 해석한 후 요청의 종류에 따라 접근제어 수단 또는 인증 수단 또는 외부의 공개키 기반 구조 인증 서버로 처리를 요청하기 위한 XML 키 관리 수단; 상기 XML 키 관리 수단으로부터의 공유 보안 정보 처리 요청에 따라 사용자 인증 기능, 제한공유 데이터 저장 수단에 대한 접근 권한 정책 생성 기능, 접근 권한 정책에 따른 접근 권한 확인 기능, 접근이 허용된 사용자에게 공유 보안 정보 제공 기능, 보안 정보 위치 정보 제공 기능, 공유 보안 정보의 등록/삭제/갱신 기능, 공유 보안 정보에 대한 공유 설정/해제 기능, 및 XML 전자서명/검증/암호화/복호화/통신 보안 기능을 제공하기 위한 상기 접근제어 수단; 상기 XML 키 관리 수단으로부터의 비공유 보안 정보 처리 요청에 따라 사용자 인증 기능, 본인 인증 기능, 접근이 허용된 사용자(본인)에게 비공유 보안 정보 제공 기능, 보안 정보 위치 제공 기능, 비공유 보안 정보의 등록/수정/삭제 기능, 및 XML 전자서명/검증/암호화/복호화 통신 보안 기능을 제공하기 위한 상기 인증 수단; 상기 접근제어 수단의 제어에 따라 제한된 대상에게 공유되는 보안 정보를 저장하고 관리하기 위한 상기 제한공유 데이터 저장 수단; 및 상기 인증 수단의 제어에 따라 공유되어서는 안되는 보안 정보를 저장하고 관리하기 위한 비공유 데이터 저장 수단을 포함한다.

<28> 한편, 본 발명은, 보안 정보 통합 관리 방법에 있어서, 보안 정보 통합 관리 시스템이 보안 정보 통합 관리 클라이언트로부터의 보안 정보 등록/갱신/삭제 요청에 따라 보안 정보를 그 종류에 따라 분류하여 제한공유 데이터 저장소 또는 비공유 데이터 저장소에 등록/갱신/삭제하는 보안 정보 등록/갱신/삭제 단계; 상기 보안 정보 통합 관리 시스템이 상기 보안 정보

통합 관리 클라이언트로부터의 보안 정보 공유 설정/해제 요청에 따라 제한공유 데이터 저장소에 등록된 보안 정보에 대하여 공유 설정/해제하고 보안 접근 권한 정책을 생성/갱신하는 보안 정보 공유 설정/해제 단계; 상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 공유 보안 정보 제공 요청에 따라 상기 보안 접근 권한 정책에 따른 요청 사용자의 권한을 확인한 후, 해당 보안 정보를 상기 보안 정보 통합 관리 클라이언트로 제공하는 공유 보안 정보 제공 단계; 상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 비공유 보안 정보 제공 요청에 따라 요청 사용자가 비공유 보안 정보의 소유주임을 인증한 후, 해당 보안 정보를 상기 보안 정보 통합 관리 클라이언트로 제공하는 비공유 보안 정보 제공 단계; 및 상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 XML을 이용한 전자서명 생선/검증 요청에 따라 전자서명을 생성/검증하는 전자서명 생성/검증 단계를 포함한다.

<29> 이 때, 본 발명에 따른 보안 정보 통합 관리 시스템은 다수 존재할 수 있으며, 사용자는 자신의 보안 정보를 여러 보안 정보 관리 시스템에 분산하여 관리할 수 있다.

<30> 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

<31> 도 1은 본 발명에 따른 보안 정보 통합 관리 시스템의 일실시예 구성도이다.

<32> 우선, 본 발명에 따른 보안 정보 통합 관리 시스템(13)은 종래의 보안 정보 관리 도구들의 문제점을 해결하기 위한 것으로서, 공개키기반구조(PKI) 및 XML 키 관리 스펙(XKMS)을 기반으로 하여 다양한 보안 정보를 통합적으로 관리하고, 온라인 및 오프라인에서의 보안 정보를 XML 국제 표준에 맞도록 변환하여 관리한다.

<33> 한편, 확장 XKMS 클라이언트(11)는 종래의 XKMS 클라이언트의 기능을 확장한 것으로서, 기존의 인증서 및 개인키에 관한 관리 기능 이외에 비밀키, 속성 인증서, 패스워드, 패스프레이즈, 웹서비스 보안 토큰 등의 보안 정보를 관리할 수 있다. 그 확장된 기능들은 다음과 같다.

<34> 1) 보안 정보 위치 정보 제공 기능 : 보안 정보가 저장된 위치를 제공하는 기능.

<35> 2) 보안 정보 등록 기능 : 보안 정보를 저장소에 저장하는 기능.

<36> 3) 보안 정보 공유 설정/해제 요청 기능 : 제한공유 데이터 저장소(134)에 저장된 보안 정보에 대하여 공유 설정/해제를 요청하는 기능.

<37> 4) 보안 정보 공유 대리 설정 기능 : 제한공유 데이터 저장소(134)에 저장된 보안 정보에 대하여 소유주의 서명을 받아 타 사용자가 공유 설정/해제할 수 있도록 하는 기능.

<38> 5) 보안 정보 공유 대리 설정 확인 기능 : 타 사용자로부터의 보안 정보 공유 대리 설정 요청을 보안 정보 소유주에게 알리는 기능.

<39> 6) 보안 정보 수정 기능 : 제한공유 데이터 저장소(134) 및 비공유 데이터 저장소(135)에 저장되어 있는 보안 정보를 수정할 수 있는 기능.

<40> 7) 공유 보안 정보 요청 기능 : 타 소유주에 의하여 공유된 보안 정보에 접근을 요청하는 기능.

<41> 8) 보안 정보 검증 요청 기능 : 특정 형태로 인코딩된 타 소유주 보안 정보에 대한 검증을 확장 XKMS 서버(131)로 요청하는 기능으로서, 확장 XKMS 서버(131)에 보안 정보 검증을 요청시에는 타 소유주의 보안 정보 검증 요청 확인 과정을 거쳐야 함.

<42> 9) 보안 정보 검증 요청 확인 기능 : 타 사용자로부터 자신이 소유한 보안 정보에 대한 검증 요청이 발생하였음을 알리는 기능.

<43> 10) 보안 정보 저장 기능 : 제한공유 데이터 저장소(134) 또는 비공유 데이터 저장소(135)에 저장되어 있는 보안 정보를 동일한 형태로 저장하는 기능.

<44> 11) 보안 정보 생성 기능 : 다양한 보안 정보를 생성하는 기능 및 확장 XKMS 서버(131)에 보안 정보 생성을 요청하는 기능.

<45> 12) 보안 정보 변환 기능 : 다양한 형태의 보안 정보를 XML 형태로 변환하고, XML 형태의 보안 정보를 특정 형태로 변환하는 기능.

<46> 13) 공유 보안 정보 이용 로그 확인 기능 : 제한공유 데이터 저장소(134)에 저장되어 있는 공유 보안 정보 이용에 대한 로그를 확인하는 기능.

<47> 14) 공유 보안 정보 검색 기능 : 타 사용자로부터 발급받은 서명 및 인증서를 이용하여 자신에게 공유된 보안 정보를 검색하는 기능.

<48> 15) 공유 보안 정보 검색 확인 기능 : 공유 보안 정보 검색 기능 실행에 따라 해당 타 사용자에게 이를 알리는 기능.

<49> 16) XML 전자서명/검증/암호화/복호화/통신 보안 기능 : XML을 이용한 전자서명/검증 기능, 암호화/복호화 기능, 및 통신 보안 기능.

<50> 이상에서 상술한 것과 같은 확장 XKMS 클라이언트(11)의 기능은, XKMS 서버(131)로의 요청에 의하여 실행되며, 요청에 따른 실질적인 처리는 접근제어 서버(132) 또는 인증 서버(133)에서 이루어진다.

<51> 한편, 본 발명에 따른 보안 정보 통합 관리 시스템(13)은, 확장 XKMS 서버(131), 접근제어 서버(132), 인증 서버(133), 제한공유 데이터 저장소(134), 및 비공유 데이터 저장소(135)를 포함한다.

<52> 상기 확장 XKMS 서버(131)는 확장 XKMS 클라이언트(11)와 PKI 인증 서버(12) 사이에서 인증서 및 개인키에 관련된 프로세스는 종래와 같이 처리하고, 그 이외의 보안 정보(패스워드(패스프레이즈), 웹서비스의 보안 토큰, 생체 정보 등)는 그 종류에 따라 접근제어 서버(132) 또는 인증 서버(133)에서 처리되며, 제한공유 데이터 저장소(134) 또는 비공유 데이터 저장소(135)에 저장된다.

<53> 즉, 상기 확장 XKMS 서버(131)는 확장 XKMS 클라이언트(11)와 PKI 인증 서버(12) 사이에서 보다 쉬운 사용자 인터페이스를 제공하도록 설계된 XML 키 관리 스펙(XKMS)을 확장한 것으로서, 사용자는 확장 XKMS 클라이언트(11)를 통하여 XML로 인터페이스하고, 확장 XKMS 서버(131)가 XML 인터페이스와 PKI 인터페이스를 상호 변환하여 확장 XKMS 클라이언트(11)와 PKI 인증 서버(12)가 서로 인터페이스되도록 한다. 이 때, 확장 XKMS 서버(131)는 공개키기반구조(PKI)의 인증서 및 개인키는 물론 비밀키, 속성 인증서, 패스워드(패스프레이즈), 웹서비스의 보안 토큰, 생체 정보 등의 보안 정보를 관리하기 위하여 종래의 XML 키 관리 스펙(XKMS)을 확장하여 사용하는데, 그 상세한 확장 기능은 다음과 같다.

<54> 1) 클라이언트 요청 분류 기능 : 확장 XKMS 클라이언트(11)로부터의 요청을 해석하여, PKI 인증 서버(12) 또는 접근제어 서버(132) 또는 인증 서버(133)로 전달하는 기능.

<55> 2) 보안 정보 생성 기능 : 확장 XKMS 클라이언트(11)로부터의 요청에 따라 보안 정보를 생성하는 기능.

<56> 3) 보안 정보 변환 기능 : 확장 XKMS 클라이언트(11)로부터 전달받은 다양한 형태의 보안 정보를 XML 형태로 변환하고, XML 형태의 보안 정보를 특정 형태로 변환하는 기능.

<57> 4) XML 전자서명/검증/암호화/복호화/통신 보안 기능 : XML을 이용한 전자서명/검증 기능, 암호화/복호화 기능, 및 통신 보안 기능.

<58> 이상에서 상술한 것과 같은 기능을 가지는 확장 XKMS 서버(131)는, 확장 XKMS 클라이언트(11)로부터의 요청을 PKI 프로토콜로 변환한 후 PKI 인증 서버(12)로 전달하기도 하고, 접근제어 서버(132) 또는 인증 서버(133)로 전달하기도 한다.

<59> 또한, 확장 XKMS 서버(131)는 필요에 따라 새로운 보안 정보의 관리를 추가할 수 있다. 즉, 새로운 XML 보안 표준의 제정에 따라 또는 새로운 XML 보안 정보의 관리 필요성에 따라 새로운 보안 정보를 관리하도록 그 기능을 추가할 수 있다. 이 때, 추가되는 보안 정보는 XML 형태이며, 그 종류에 따라 제한공유 데이터 저장소(134) 또는 비공유 데이터 저장소(135)에 저장된다. 사용자의 입장에서 보면 새로운 XML 보안 정보의 추가가 기존의 인터페이스에 미치는 영향은 없다. 왜냐하면, 확장 XKMS 서버(131)가 확장 XKMS 클라이언트(11)로부터 전달받은 보안 정보를 그 타입에 따라 분류하여 접근제어 서버(132) 또는 인증 서버(133)에 처리를 요청하기 때문에, 확장 XKMS 서버(131)의 기능을 확장하는 것 만으로 새로운 보안 정보를 추가할 수 있다.

<60> 한편, 제한공유 데이터 저장소(134)는 비밀키, 패스워드, 패스프레이즈, 및 공개 필요성이 있는 웹서비스 보안 토큰 등과 같이 제한된 대상에게만 공개되는 보안 정보들을 저장하고 있으며, 인증서 및 속성 인증서도 저장하고 있다.

<61> 또한, 비공유 데이터 저장소(135)는 개인키, 생체정보 및 공개되어서는 안되는 웹서비스 보안 토큰 등과 같이 공유될 수 없는 보안 정보를 저장하고 있다.

<62> 이 때, 제한공유 데이터 저장소(134) 및 비공유 데이터 저장소(135)에 저장되는 보안 정보는 XML 암호화 후 저장되며, 경우에 따라서는 암호화되지 않고 단순히 XML로 기술되어 저장될 수도 있다. XML 암호화는 확장 XKMS 클라이언트(11)에서 이루어지거나 확장 XKMS 클라이언트(11)로부터의 요청에 따라 확장 XKMS 서버(131)에서 이루어진다. XML 복호화 역시 확장 XKMS 클라이언트(11) 또는 확장 XKMS 서버(131)에서 이루어질 수 있다. 또한, 제한공유 데이터 저장소(134) 및 비공유 데이터 저장소(135)에 저장되어 있는 보안 정보는 사용자(확장 XKMS 클라이언트)로부터의 요청에 따라 제공될 수 있다.

<63> 한편, 접근제어 서버(132)는 제한공유 데이터 저장소(134)에 대한 접근 권한을 설정하는 역할을 하며, 다음과 같은 기능을 가지고 있다.

<64> 1) 사용자 인증 기능.

<65> 2) 제한공유 데이터 저장소(134)에 대한 접근 권한 정책 생성 기능.

<66> 3) 접근 권한 정책에 따른 접근 권한 확인 기능.

<67> 4) 접근이 허용된 사용자에게 공유 보안 정보 제공 기능.

<68> 5) 보안 정보 위치 정보 제공 기능.

<69> 6) 공유 보안 정보 등록/수정/삭제 기능.

<70> 7) 공유 보안 정보에 대한 공유 설정/해제 기능.

<71> 8) 보안 정보 공유 대리 설정/확인 기능.

<72> 9) 보안 정보 검증 기능.

<73> 10) 보안 정보 검증 요청 확인 기능.

<74> 11) 보안 정보 저장/생성/변환 기능.

<75> 12) 공유 보안 정보 이용 로그 확인 기능.

<76> 13) 공유 보안 정보 검색 기능.

<77> 14) 공유 보안 정보 검색 요청 확인 기능.

<78> 15) XML 전자서명/검증/암호화/복호화/통신 보안 기능.

<79> 상술한 바와 같이, 접근제어 서버(132)는 제한공유 데이터 저장소(134)에 대한 접근을 통제하는 기능을 담당하며, 사용자 인증 및 보안 정보에 대한 인가를 담당한다. 이 때, 사용자 인증은 공개키기반구조(PKI)를 사용하며, 보안 정보에 대한 인가는 접근 권한 정책에 따라 결정한다. 즉, 접근제어 서버(132)는 확장 XKMS 클라이언트(11)로부터 제한공유 데이터 저장소(134)에 대한 접근 요청을 전달받으면 우선 사용자 인증을 거친 후, 해당 보안 정보에 상응하는 접근 권한 정책을 읽어들여 사용자에게 권한이 있는지를 확인한다. 그리고, 사용자가 권한이 있는 경우에만 제한공유 데이터 저장소(134)에 저장된 보안 정보를 제공해 주게 된다.

<80> 이 때, 접근 권한 정책은 사용자가 확장 XKMS 클라이언트(11)를 통하여 보안 정보를 제한공유 데이터 저장소(134)에 저장하거나 특정 사용자가 접근할 수 있도록 공유를 요청하였을 때 생성되고, 지속적이고 동적으로 관리된다. 즉, 접근제어 서버(132)가 확장 XKMS 클라이언트(11)를 통하여 전달받은 보안 정보 등록/수정/삭제/공유 설정 및 해제 등의 요청에 따라 접근 권한 정책을 업데이트하여 저장한다. 따라서, 접근제어 서버(132)에서의 접근 권한 정책은 통상적인 접근제어 시스템처럼 별도의 관리자가 작성하는 것이 아니라, 접근제어 서버(132)가 미리 정해진 규칙에 따라 사용자로부터의 요청에 따라 생성된다.

<81> 또한, 접근제어 서버(132)는 종래의 인증서, 속성 인증서 등과 같이 누구에게나 공개되어도 상관없는 보안 정보를 무제한 공유 데이터 저장소(121)에 저장한다. 이 때, 무제한 공유 데이터 저장소(121)는 PKI 인증 서버(12)의 디렉토리에 포함시킬 수 있다. 물론, 종래의 PKI 인증 서버(12)의 디렉토리는 저장될 수 있는 보안 정보가 인증서로 한정되어 있기 때문에 다른 종류의 보안 정보를 저장할 수 있도록 확장시켜야 한다.

<82> 한편, 인증 서버(133)는 비공유 데이터 저장소(135)에 대한 접근을 통제하는 역할을 담당하며, 다음과 같은 기능을 수행한다.

<83> 1) 사용자 인증 기능.

<84> 2) 본인 인증 기능.

<85> 3) 접근 권한 결과 작성 기능.

<86> 4) 접근이 허용된 사용자에게 보안 정보 제공 기능.

<87> 5) 보안 정보 등록/수정/삭제 기능.

<88> 6) 보안 정보 검증 기능.

<89> 7) 보안 정보 검증 요청 확인 기능.

<90> 8) 보안 정보 위치 제공 기능.

<91> 9) 보안 정보 저장 기능.

<92> 10) 보안 정보 검색 기능.

<93> 11) XML 전자서명/검증/암호화/복호화/통신 보안 기능.

<94> 상술한 바와 같이, 인증 서버(133)는 비공유 데이터 저장소(135)에 대한 접근을 통제하는 서버로서, 접근하려는 사용자에 대한 인증을 담당한다. 특히, 비공유 데이터 저장소(135)에

는 공유되어서는 안되는 중요한 보안 정보가 저장되어 있으며, 소유주 본인에게만 공개되어야 하기 때문에, 인증 서버(133)는 접근을 요청하는 사용자가 소유주 본인인지를 인증하여야 한다. 즉, 인증 서버(133)에서의 사용자 인증 기능은 사용자를 인증하는 기능이고, 본인 인증 기능은 접근하려는 보안 정보가 사용자 본인의 소유인지를 확인하는 기능이다.

<95> 도 2는 본 발명에 따른 제한공유 데이터 저장소에 대한 일실시예 구조도이다.

<96> 도 2에 도시된 바와 같이, 본 발명에 따른 제한공유 데이터 저장소(134)는, 각 사용자별, 타입별로 구별된 보안 정보 및 보안 정보 형태를 포함한다. 즉, 사용자 별로 인증서, 비밀키, 속성 인증서, 패스워드, 패스 프레이즈 및 공유 가능한 웹 서비스 보안 토큰 등의 보안 정보가 타입별로 저장되어 있으며, 각 보안 정보에 상응하는 보안 정보 형태가 저장되어 있다. 보안 정보 형태는 제한공유 데이터 저장소(134)에 실제적으로 저장된 보안 정보의 형태에 관한 정보로서, 도 2에 도시된 바와 같이, 암호화되어 저장되는 것도 있고, 암호화되지 않은 형태의 보안 정보 그 자체로 저장되는 것도 있다.

<97> 예를 들어, 인증서(21)의 경우에는 인증서의 XML 타입인 "X509Certificate"(211) 형태로 저장되고, 비밀키(22)의 경우에는 암호화되어 "EncryptedKey"(221) 형태로 저장된다. 단, 저장되는 보안 정보는 XML 형태를 기본으로 하며, "W3C" 혹은 "OASIS" 등에서 제정한 국제적인 XML 표준에 따른다.

<98> 도 3은 본 발명에 따른 비공유 데이터 저장소에 대한 대한 일실시예 구조도이다.

<99> 도 3에 도시된 바와 같이, 본 발명에 따른 비공유 데이터 저장소(135)는, 제한공유 데이터 저장소(134)와 마찬가지로, 각 사용자별, 타입별로 구별된 보안 정보 및 보안 정보 형태를 포함한다. 즉, 사용자별로 공유할 수 없는 개인키, 생체 정보, 공유할수 없는 웹서비스 보안

토큰 등이 저장되어 있으며, 그 저장 형태는 "EncryptedKey" 또는 "EncryptedData" 등과 같은 XML 형태이다. 참고로, "EncryptedKey" 및 "EncryptedData"는 모두 "W3C"에서 정의한 XML 암호화(Encryption)의 한 엘리먼트로서 암호화되었다는 것을 나타내며, 암호화된 내용이 키 일 경우에는 "EncryptedKey" 엘리먼트가, 암호화된 내용이 데이터일 경우에는 "EncryptedData"가 사용된다.

<100> 한편, 본 발명에 따른 보안 정보 통합 관리 시스템의 전체적인 동작 과정을 살펴보면 다음과 같다.

<101> 먼저, 사용자는 종래의 방식대로 PKI 인증 서버(12)에 등록과정을 통하여 한쌍의 공개키 쌍을 디렉토리에 저장한다. 이후로 사용자는 확장 XKMS 서버(131)를 통하여 자신의 공개키 쌍을 갱신하거나 취소할 수 있다.

<102> 한편, 사용자는 확장 XKMS 서버(131)를 통하여 보안 정보 등록/갱신/공유 등의 서비스를 요청할 수 있으며, 확장 XKMS 서버(131)는 사용자로부터의 요청에 따라 사용자 인증을 거친 후 서비스를 요청받은 보안 정보의 종류에 따라 PKI 인증 서버(12), 접근제어 서버(132) 또는 인증 서버(133)로 해당 서비스를 요청하게 된다.

<103> 이 때, 보안 정보 공유 서비스를 요청받은 접근제어 서버(132)는 요청 사용자의 인증서를 PKI 인증 서버(12)로부터 읽어들여 유효성 등을 재차 확인한다. 그리고, 정당한 사용자임을 확인한 후에 제한공유 데이터 저장소(134)로부터 해당 공유 보안 정보를 읽어들인 후, 확장 XKMS 서버(131)로 전달하면 확장 XKMS 서버(131)는 읽어들인 보안 정보를 확장 XKMS 클라이언트(11)를 통하여 요청 사용자에게 전송한다.

<104> 보다 상세한 과정에 대하서는 도 4 내지 도 7을 참조하여 보다 상세히 살펴보기로 한다.

<105> 도 4는 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트(11)로부터의 요청에 따른 보안 정보 등록 과정에 대한 일실시예 흐름도이다.

<106> 먼저, 사용자가 확장 XKMS 클라이언트(11)를 통하여 보안 정보의 저장을 요청하면(401), 확장 XKMS 서버(131)가 요청 사용자를 인증하고(402), 보안 정보의 종류를 확인한다(403,404).

<107> 상기 확인 결과(403,404), 보안 정보의 종류가 XML 암호화 데이터이면 접근제어 서버(132) 또는 인증 서버(133)로 전달하여 제한공유 데이터 저장소(134) 또는 비공유 데이터 저장소(135)에 저장되도록 한다(408).

<108> 한편, 상기 확인 결과(403,404), 보안 정보의 종류가 XML 암호화 데이터가 아니면 XML 암호화가 필요한지를 판단하여(405), XML 암호화가 필요하면 XML 암호화 파라미터를 설정하여(406) 보안 정보를 암호화한 후(407) 접근제어 서버(132) 또는 인증 서버(133)로 전달하여 제한공유 데이터 저장소(134) 또는 비공유 데이터 저장소(135)에 저장되도록 하고(408), XML 암호화가 필요하지 않으면 접근제어 서버(132) 또는 인증 서버(133)로 전달하여 제한공유 데이터 저장소(134) 또는 비공유 데이터 저장소(135)에 저장되도록 한다(408). 이 때, XML 암호화 필요성 여부는 사용자가 보안 정보 저장 요청시에 선택적으로 요청한다.

<109> 도 5는 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 공유 설정/해제 과정에 대한 일실시예 흐름도이다.

<110> 먼저, 사용자가 확장 XKMS 클라이언트(11)를 통하여 자신이 소유한 보안 정보의 공유 설정/해제를 요청하면(501), 확장 XKMS 서버(131)가 요청 사용자를 인증하고(502), 공유 설정/해제를 요청한 보안 정보를 확인한 후(503), 공유자의 인증서를 확인한다(504).

<111> 이후, 공유 설정/해제를 요청한 보안 정보에 대한 접근 권한 정책을 생성하거나 또는 갱신한 후(505) 저장한다(506). 이 때, 생성 또는 갱신된 접근 권한 정책은 제한공유 데이터 저장소(134)의 접근을 통제하는 접근제어 서버(132)에 저장되며, 접근 권한 정책에 설정된 공유자만이 해당 보안 정보에 접근할 수 있는 권한을 갖게 된다.

<112> 도 6은 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 공유 과정에 대한 일실시예 흐름도이다.

<113> 먼저, 사용자가 확장 XKMS 클라이언트(11)를 통하여 보안 정보에 대한 공유를 요청하면(601), 확장 XKMS 서버(131)가 요청 사용자를 인증하고(602), 접근제어 서버(132)가 공유를 요청한 보안 정보에 대한 접근 권한 정책을 로딩한 후(603), 접근 권한 정책에 요청 사용자가 공유를 허용하도록 설정되어 있는지 확인한다(604).

<114> 상기 확인 결과(604), 공유를 허용하도록 설정되어 있으면 보안 정보가 XML 암호화 데이터인지를 확인하여(605), 보안 정보가 XML 암호화 데이터가 아니면 "609" 과정으로 진행하여 보안 정보를 확장 XKMS 클라이언트(11)를 통하여 요청 사용자에게 전송하고(609), 보안 정보가 XML 암호화 데이터이면 복호화 요청이 있었는지를 확인하여(606), 복호화 요청이 있었으면 복호화 파라미터를 설정하여(607) 복호화한 후(608) 보안 정보를 확장 XKMS 클라이언트(11)를 통하여 요청 사용자에게 전송한다(609). 그리고, 복호화 요청이 없었으면 "609" 과정으로 진행하여 보안 정보를 확장 XKMS 클라이언트(11)를 통하여 요청 사용자에게 전송한다(609).

<115> 한편, 상기 확인 결과(604), 공유를 허용하도록 설정되어 있지 않으면 확장 XKMS 클라이언트(11)를 통하여 요청 사용자에게 공유가 거부되었음을 알린다(610).

<116> 한편, 사용자는 보안 정보 공유 요청시에 XML 암호화된 데이터 자체 또는 복호화된 데이터를 선택적으로 요청할 수 있다.

<117> 도 7은 본 발명에 따른 보안 정보 통합 관리 시스템에서 확장 XKMS 클라이언트로부터의 요청에 따른 보안 정보 갱신 과정에 대한 일실시예 흐름도이다.

<118> 먼저, 사용자가 확장 XKMS 클라이언트(11)를 통하여 자신이 소유한 보안 정보의 갱신을 요청하면(701), 확장 XKMS 서버(131)가 요청 사용자를 인증하고(702), 갱신을 요청한 보안 정보를 확인한 후(703), 갱신한다(704).

<119> 이상에서 살펴본 바와 같이, 본 발명에 따른 보안 정보 통합 관리 시스템은 다양한 보안 정보들을 통합적으로 관리할 수 있으며, 모든 보안 정보를 XML 기반의 국제 표준에 따라 관리함으로써 보안 정보의 호환성 문제를 해결할 수 있는 효과가 있다.

<120> 예를 들어, 사용자가 확장 XKMS 클라이언트(11)를 통하여 생체 정보의 등록을 보안 정보 통합 관리 시스템(13)에 요청하면, 보안 정보 통합 관리 시스템(13)은 사용자 인증 후에 사용자로부터 입력받은 생체정보를 사용자가 선택한 인코딩 알고리즘과 키로 인코딩한 후 비공유 데이터 저장소(135)에 저장한다.

<121> 그러면, 사용자는 생체 정보를 이용하여 인증을 수행하는 서비스 제공자가 생체 정보를 요청시에 자신의 생체 정보를 인코딩 알고리즘과 키로 인코딩한 후 타임 스탬프 등과 함께 서명하여 상기 서비스 제공자 측에 전달한다.

<122> 그러면, 상기 서비스 제공자는 보안 정보 통합 관리 시스템(13)에 사용자로부터 전달받은 암호화된 생체 정보의 인증을 요청하고, 보안 정보 통합 관리 시스템(13)은 확장 XKMS 클라이언트(11)를 통하여 사용자에게 생체 정보의 인증을 요청받았음을 알린 후, 사용자 확인에 따

라 비공유 데이터 저장소(135)에 저장되어 있는 암호화된 생체 정보와 비교하여 그 결과를 상기 서비스 제공자 측에 통보한다.

<123> 이 때, 사용자는 생체 정보를 암호화하는 인코딩 알고리즘과 키를 다양하게 선택할 수 있기 때문에 타인에 의하여 발생할 수 있는 생체 정보의 오용을 방지할 수 있는 효과가 있다.

<124> 이와 같은 생체 정보를 이용한 인증은 여권이나 비자에 이용할 수 있을 것이다. 즉, 여권의 경우에 사용자는 국가에서 인정하는 인증 기관 또는 인증 대행 업체에서 생체 정보를 추출한 후 상대 국가가 공인하는 알고리즘 및 키를 이용하여 인코딩한 다음, 상대 국가의 공인인증기관(예를 들어, 출입국 관리국)에서 운영하는 보안 정보 통합 관리 시스템(13)의 비공유 데이터 저장소(135)에 등록한다.

<125> 그러면, 상대 국가에서는 상기 사용자에 대한 출입국 관리시에 상기 사용자의 생체 정보가 등록된 보안 정보 통합 관리 시스템(13)을 이용하여 생체 정보 인증을 할 수 있게 된다. 비자의 경우에도 같은 방법을 적용할 수 있다.

<126> 한편, 본 발명은, 패스워드 및 패스프레이즈 등과 같이 사용자 인증에 많이 사용되는 보안 정보를 제한공유 데이터 저장소(134)에 저장하여 로인인 과정을 생략하거나 싱글 사인 온(SSO : Single Sing On)에 활용할 수 있다. 싱글 사인 온(SSO)은 다양한 업무 시스템의 인증 정보를 하나의 단일 계정으로 통합하여 단 한번의 로그인으로 복수의 업무시스템을 동시에 사용할 수 있게 하는 기술이다.

<127> 즉, 사용자는 서비스 제공자의 인증요구에 따라 패스워드 또는 패스프레이즈에 대한 위치 정보에 대하여 서명하면, 서비스 제공자는 서명을 인증한 후, 사용자로부터 입력받은 위치 정보를 이용하여 패스워드 또는 패스프레이즈(공유할 보안

정보)에 공유를 설정하고, 서비스 제공자의 URL, 인증서 등의 정보를 제한공유 데이터 저장소(134)에 저장한다(보안 정보 공유 대리 설정 기능). 이 때, 서비스 제공자는 사용자가 등록하지 않은 관련 사이트들을 다수 등록할 수 있으며, 사용자는 확장 XKMS 클라이언트(11)를 통하여 상기 서비스 제공자의 보안 정보 공유 대리 설정을 통보받을 수 있다. 그러면, 이후로 사용자는 보안 정보 공유 대리 설정 기능에 의하여 패스워드 또는 패스프레이즈의 공유가 설정된 사이트에 회원가입 또는 로그인 과정을 생략할 수 있게 된다. 이 때, 인증 및 승인을 위한 정보를 XML로 인코딩하고 교환할 수 있도록 하는 보안 표준인 보안 지정 마크업 언어(SAML : Security Assertion Markup Language)를 이용하면 더 자연스러운 싱글 사인 온(SSO)의 운영이 가능하다.

<128> 또한, 수많은 인터넷 서비스 업체에서 회원 가입시 개인 정보를 요구하는데 그 때마다 반복해서 개인 정보를 입력하는 일은 매우 불편한 일이다. 그런데, 본 발명에 따른 보안 정보 통합 관리 시스템(13)의 제한공유 데이터 저장소(134)에 개인정보를 XML 형태로 저장하고, 인터넷 서비스 업체에 공유 설정을 해놓으면 사용자는 인터넷 서비스 업체마다 개인 정보를 입력하지 않아도 된다. 이 때, 개인 정보를 중요도에 따라 계층화하고, 각 계층에 따라 공유를 설정할 수 있다.

<129> 만약, 사용자가 가입했던 인터넷 서비스 업체로부터 탈퇴를 원할 때에는 인터넷 서비스 업체로부터 탈퇴 요구 승인 서명을 받아 비공유 데이터 저장소(135)에 저장하여, 탈퇴 이후에 발생할 수 있는 개인 정보 무단 사용 및 누출 등에 대처할 수 있도록 한다. 인터넷 서비스 업체의 약관 또한 마찬가지로 적용가능하다. 이는 월드와이드웹 컨소시움(W3C : World Wide Web Consortium)에서 정의하는 P3P(Platform for Privacy Preference)를 이용하여 구현할 수 있을 것이다.

<130> 이와 같이 구현하면 인터넷 서비스 업체 입장에서는 개인 정보 보호에 별도의 노력이 필요없으며 쉽게 사용자의 정보를 획득할 수 있는 이점이 있는 한편, 개인의 입장에서는 반복적인 개인 정보 입력을 생략할 수 있으므로 편리한 이점이 있다.

<131> 또한, 본 발명은, 비밀키를 제한공유 데이터 저장소에 저장하고, 공유가 설정된 여러 사용자가 공유할 수 있게 됨에 따라 키 분배 문제를 해결할 수 있는 효과가 있다.

<132> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

<133> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

【발명의 효과】

<134> 상기와 같이 본 발명은, 다양한 보안 정보들을 통합적으로 관리할 수 있으며, 모든 보안 정보를 XML 기반의 국제 표준에 따라 관리함으로써, 보안 정보의 호환성 문제를 해결할 수 있는 효과가 있다.

<135> 또한, 본 발명은, 비밀키를 제한공유 데이터 저장소에 저장하고, 공유가 설정된 여러 사용자가 공유할 수 있게 됨에 따라 키 분배 문제를 해결할 수 있는 효과가 있다.

<136> 또한, 본 발명은, 보안 정보의 이동성이 뛰어나고, 로그인 과정 등을 생략할 수 있어 사용자의 편리성을 향상시킬 수 있으며, 키보드의 입력을 최소화시켜 소형 무선 인터넷 기기의 활용성을 높일 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

보안 정보 통합 관리 시스템에 있어서,

외부의 보안 정보 통합 관리 클라이언트와 XML(Extensible Markup Language)을 기반으로 인터페이스하고, 사용자를 인증하며, 상기 보안 정보 통합 관리 클라이언트로부터의 요청을 해석한 후 요청의 종류에 따라 접근제어 수단 또는 인증 수단 또는 외부의 공개키 기반 구조 인증 서버로 처리를 요청하기 위한 XML 키 관리 수단;

상기 XML 키 관리 수단으로부터의 공유 보안 정보 처리 요청에 따라 사용자 인증 기능, 제한공유 데이터 저장 수단에 대한 접근 권한 정책 생성 기능, 접근 권한 정책에 따른 접근 권한 확인 기능, 접근이 허용된 사용자에게 공유 보안 정보 제공 기능, 보안 정보 위치 정보 제공 기능, 공유 보안 정보의 등록/삭제/갱신 기능, 공유 보안 정보에 대한 공유 설정/해제 기능, 및 XML 전자서명/검증/암호화/복호화/통신 보안 기능을 제공하기 위한 상기 접근제어 수단;

상기 XML 키 관리 수단으로부터의 비공유 보안 정보 처리 요청에 따라 사용자 인증 기능, 본인 인증 기능, 접근이 허용된 사용자(본인)에게 비공유 보안 정보 제공 기능, 보안 정보 위치 제공 기능, 비공유 보안 정보의 등록/수정/삭제 기능, 및 XML 전자서명/검증/암호화/복호화 통신 보안 기능을 제공하기 위한 상기 인증 수단;

상기 접근제어 수단의 제어에 따라 제한된 대상에게 공유되는 보안 정보를 저장하고 관리하기 위한 상기 제한공유 데이터 저장 수단; 및

상기 인증 수단의 제어에 따라 공유되어서는 안되는 보안 정보를 저장하고 관리하기 위한 비공유 데이터 저장 수단

을 포함하는 보안 정보 통합 관리 시스템.

【청구항 2】

제 1 항에 있어서,

상기 접근제어 수단의 접근 권한 정책에 따른 접근 권한 확인 기능은,

상기 접근제어 수단이 상기 XML 키 관리 수단으로부터 상기 제한공유 데이터 저장 수단에 대한 접근 요청을 전달받으면 사용자 인증을 거친 후, 요청한 보안 정보에 상응하는 접근 권한 정책을 읽어들여 사용자에게 권한이 있는지를 확인하는 것을 특징으로 하는 보안 정보 통합 관리 시스템.

【청구항 3】

제 2 항에 있어서,

상기 접근 권한 정책은,

사용자가 상기 보안 정보 통합 관리 클라이언트를 통하여 보안 정보를 등록시에 생성되며, 이후에 등록한 보안 정보의 갱신/삭제, 공유 설정/해제에 따라 지속적이고 동적으로 업데이트되는 것을 특징으로 하는 보안 정보 통합 관리 시스템.

【청구항 4】

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 접근제어 수단 및 인증 수단은,

상기 보안 정보 통합 관리 클라이언트의 요청에 따라 보안 정보의 소유주로부터 부여받은 서명을 이용하여 타 사용자가 공유 설정/해제할 수 있도록 하는 보안 정보 공유 대리 설정 기능 및 보안 정보의 소유주에게 보안 정보 공유 대리 설정 요청을 알리는 기능을 더 수행하는 것을 특징으로 하는 보안 정보 통합 관리 시스템.

【청구항 5】

제 4 항에 있어서,

상기 접근제어 수단 및 인증 수단은,

상기 보안 정보 통합 관리 클라이언트의 요청에 따라 타 사용자로부터 발급받은 서명 및 인증서를 이용하여 자신에게 공유된 보안 정보를 검색하는 공유 보안 정보 검색 기능, 공유 보안 정보 검색 기능 실행에 따라 보안 정보의 소유주에게 이를 알리는 공유 보안 정보 검색 확인 기능, 및 공유 보안 정보 이용에 대한 로그를 확인하는 공유 보안 정보 이용 로그 확인 기능을 더 수행하는 것을 특징으로 하는 보안 정보 통합 관리 시스템.

【청구항 6】

보안 정보 통합 관리 방법에 있어서,

보안 정보 통합 관리 시스템이 보안 정보 통합 관리 클라이언트로부터의 보안 정보 등록/갱신/삭제 요청에 따라 보안 정보를 그 종류에 따라 분류하여 제한공유 데이터 저장소 또는 비공유 데이터 저장소에 등록/갱신/삭제하는 보안 정보 등록/갱신/삭제 단계;

상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 보안 정보 공유 설정/해제 요청에 따라 제한공유 데이터 저장소에 등록된 보안 정보에 대하여 공유 설정/해제하고 보안 접근 권한 정책을 생성/갱신하는 보안 정보 공유 설정/해제 단계;

상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 공유 보안 정보 제공 요청에 따라 상기 보안 접근 권한 정책에 따른 요청 사용자의 권한을 확인한 후, 해당 보안 정보를 상기 보안 정보 통합 관리 클라이언트로 제공하는 공유 보안 정보 제공 단계;

상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 비공유 보안 정보 제공 요청에 따라 요청 사용자가 비공유 보안 정보의 소유주임을 인증한 후, 해당 보안 정보를 상기 보안 정보 통합 관리 클라이언트로 제공하는 비공유 보안 정보 제공 단계; 및

상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 XML을 이용한 전자서명 생선/검증 요청에 따라 전자서명을 생성/검증하는 전자서명 생성/검증 단계

를 포함하는 보안 정보 통합 관리 방법.

【청구항 7】

제 6 항에 있어서,

상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 타 소유주 보안 정보의 공유 대리 설정 요청에 따라 보안 정보의 소유주에게 보안 정보 공유 대리 설정 요청을 알려 승인을 받은 후, 타 사용자가 상기 보안 정보의 소유주로부터 부여받은 서명을 이용하여 해당 보안 정보의 공유를 설정/해제하도록 하는 단계

를 더 포함하는 보안 정보 통합 관리 방법.

【청구항 8】

제 6 항 또는 제 7 항에 있어서,

상기 보안 정보 통합 관리 시스템이 상기 보안 정보 통합 관리 클라이언트로부터의 타 소유주 보안 정보 검증 요청에 따라 보안 정보의 소유주에게 보안 정보 검증 요청을 알려 승인을 받은 후, 타 소유주 보안 정보를 검증한 결과를 상기 보안 정보 통합 관리 클라이언트로 제공하는 단계

를 더 포함하는 보안 정보 통합 관리 방법.

【청구항 9】

제 8 항에 있어서,

상기 보안 정보 등록/갱신/삭제 단계는,

상기 보안 정보 통합 관리 시스템의 확장 XKMS 서버가 상기 보안 정보 통합 관리 클라이언트를 통하여 사용자부터 보안 정보 등록/갱신/삭제를 요청받는 단계;

상기 확장 XKMS 서버가 요청 사용자를 인증하고, 보안 정보의 종류를 확인하는 단계

상기 확인 결과, 보안 정보의 종류가 공유 가능한 것이면 접근제어 서버로 요청을 전달하여 제한공유 데이터 저장소에 등록/갱신/삭제되도록 하는 단계;

상기 제 단계의 확인 결과, 보안 정보의 종류가 공유 불가능한 것이면 인증 서버로 요청을 전달하여 비공유 데이터 저장소에 등록/갱신/삭제되도록 하는 단계

를 포함하는 보안 정보 통합 관리 방법.

【청구항 10】

제 8 항에 있어서,

상기 보안 정보 공유 설정/해제 단계는,

상기 보안 정보 통합 관리 시스템의 확장 XKMS 서버가 상기 보안 정보 통합 관리 클라이언트를 통하여 사용자부터 보안 정보 공유 설정/해제를 요청받는 단계;

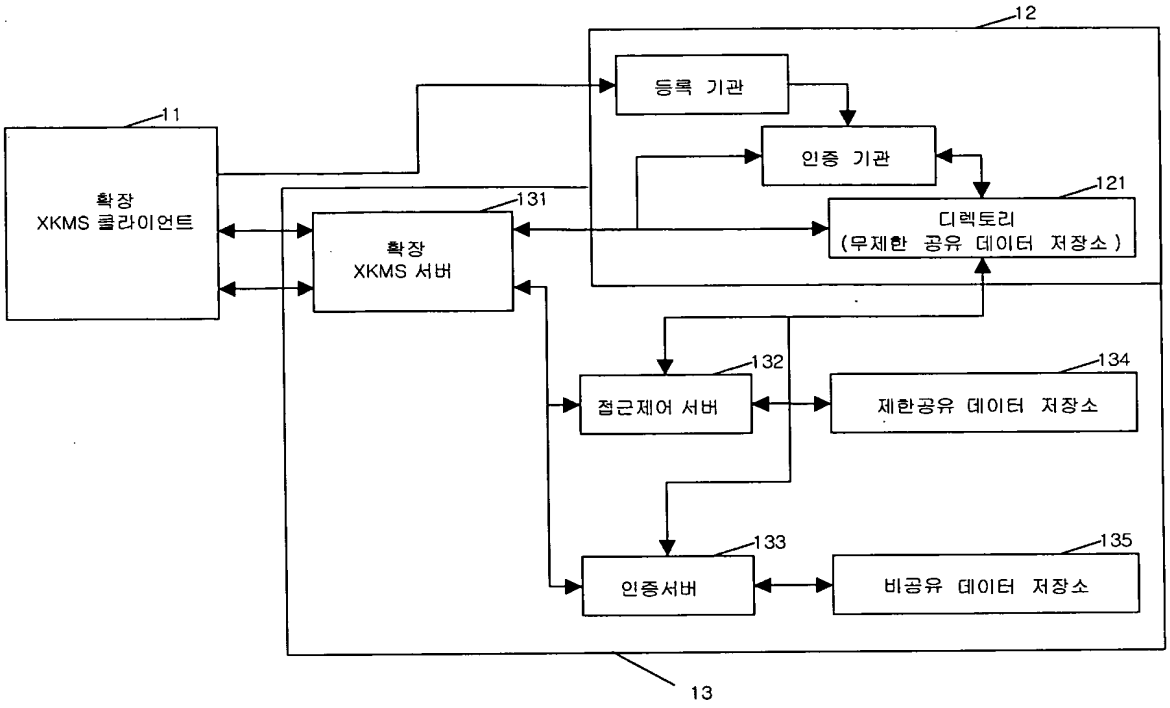
상기 확장 XKMS 서버가 요청 사용자를 인증한 후, 상기 접근제어 서버로 보안 정보 공유 설정/해제 요청을 전달하고, 상기 접근제어 서버가 해당 보안 정보에 대한 접근 권한 정책을 로딩한 후, 접근 권한 정책에 요청 사용자가 공유를 허용하도록 설정되어 있는지 확인하는 단계; 및

상기 확인 결과, 요청 사용자가 공유를 허용하도록 설정되어 있음에 따라 상기 제한공유 데이터 저장소로부터 해당 보안 정보를 읽어들여 상기 보안 정보 통합 관리 클라이언트를 통하여 요청 사용자에게 전송하는 단계

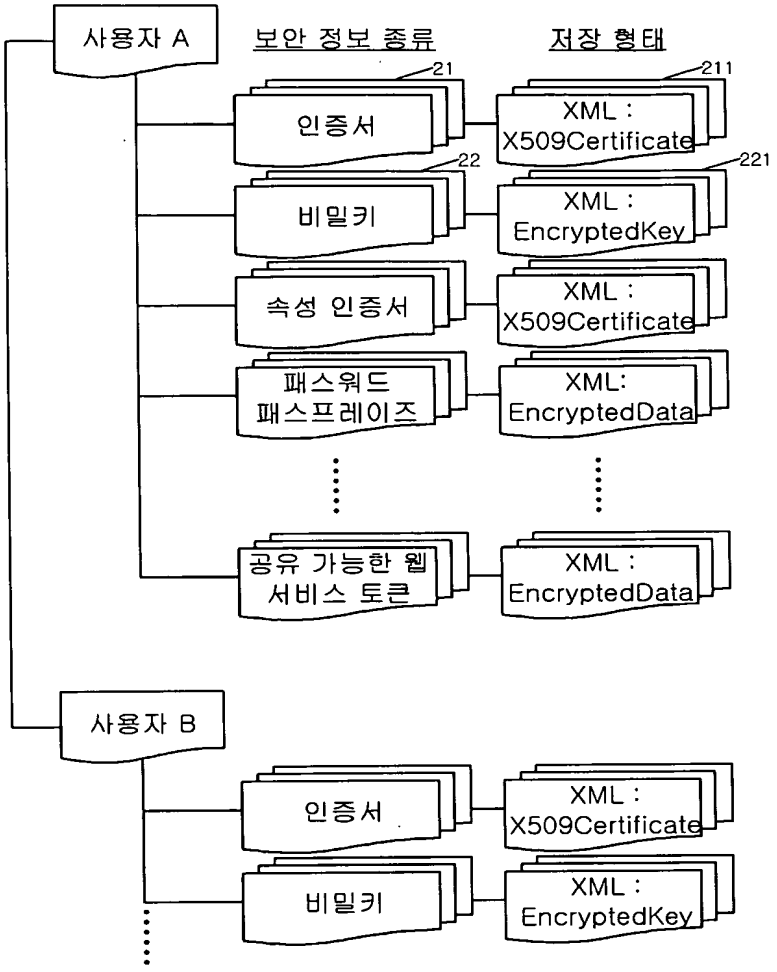
를 포함하는 보안 정보 통합 관리 방법.

【도면】

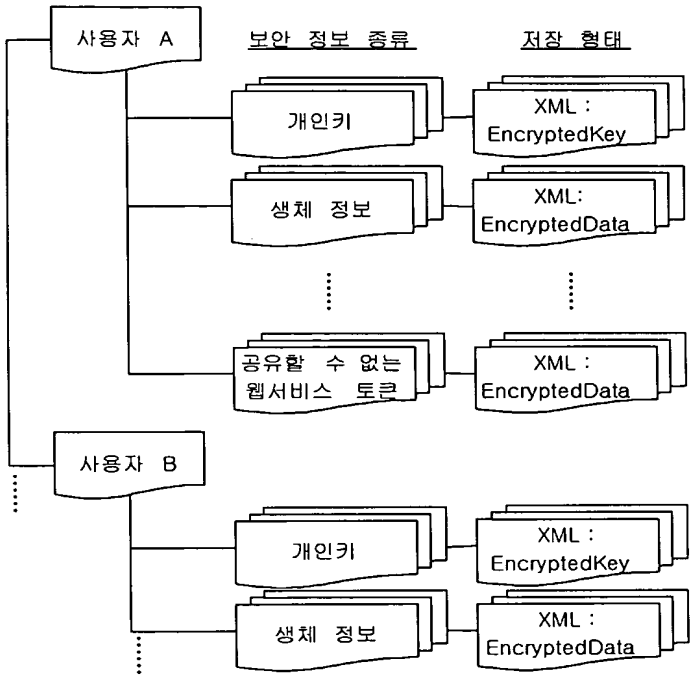
【도 1】


12
등록 기관
11
인증 기관
121
확장
XKMS 클라이언트
131
확장
XKMS 서버
디렉토리
(무제한 공유 데이터 저장소)
132
134
접근제어 서버
제한공유 데이터 저장소
133
135
인증서버
비공유 데이터 저장소
13

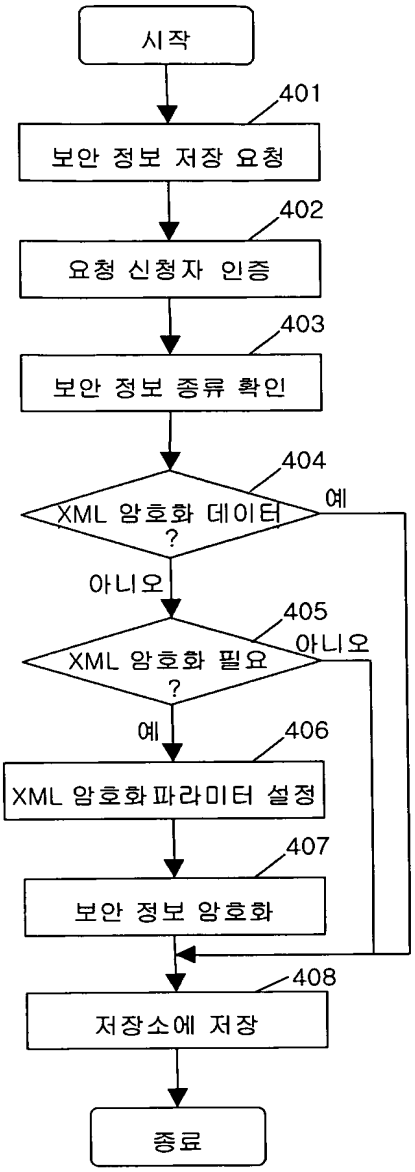
【도 2】


사용자 A
보안 정보 종류
저장 형태
21
211
인증서
XML :
X509Certificate
22
221
비밀키
XML :
EncryptedKey
속성 인증서
XML :
X509Certificate
패스워드
패스프레이즈
XML:
EncryptedData
공유 가능한 웹
서비스 토큰
XML :
EncryptedData
사용자 B
인증서
XML :
X509Certificate
비밀키
XML :
EncryptedKey

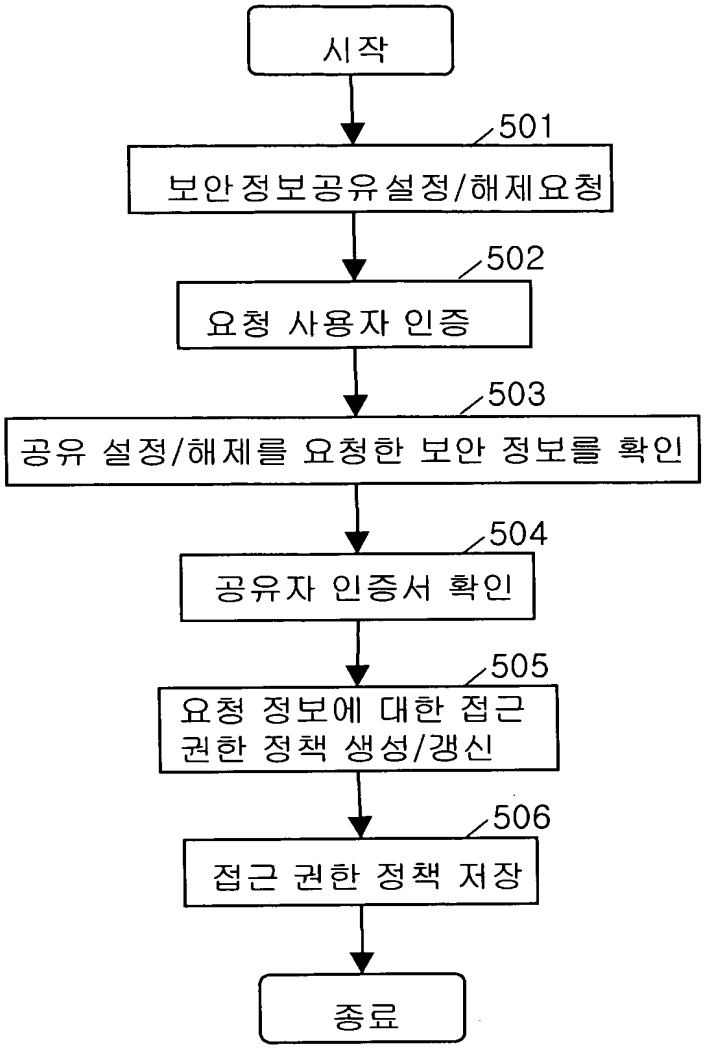
【도 3】


사용자 A
보안 정보 종류
저장 형태
개인키
XML : EncryptedKey
생체 정보
XML: EncryptedData
공유할 수 없는 웹서비스 토큰
XML : EncryptedData
사용자 B
개인키
XML : EncryptedKey
생체 정보
XML : EncryptedData

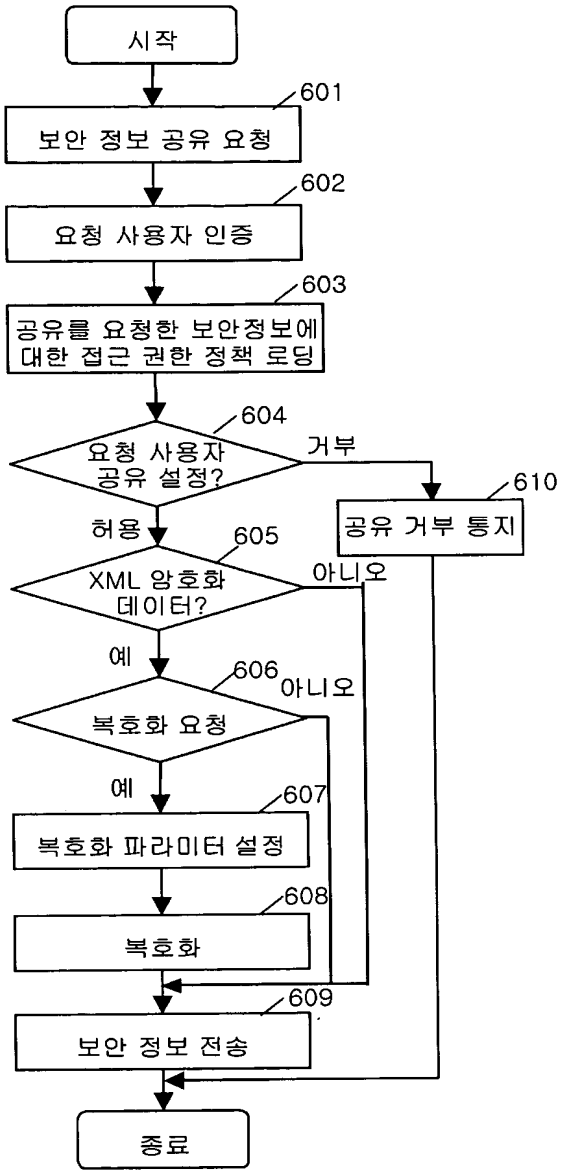
【도 4】


시작
401
보안 정보 저장 요청
402
요청 신청자 인증
403
보안 정보 종류 확인
404
XML 암호화 데이터 ?
예
아니오
405
XML 암호화 필요 ?
아니오
예
406
XML 암호화파라미터 설정
407
보안 정보 암호화
408
저장소에 저장
종료

【도 5】


시작
501
보안정보공유설정/해제요청
502
요청 사용자 인증
503
공유 설정/해제를 요청한 보안 정보를 확인
504
공유자 인증서 확인
505
요청 정보에 대한 접근 권한 정책 생성/갱신
506
접근 권한 정책 저장
종료

【도 6】


시작
601
보안 정보 공유 요청
602
요청 사용자 인증
603
공유를 요청한 보안정보에 대한 접근 권한 정책 로딩
604
요청 사용자 공유 설정?
거부
610
공유 거부 통지
허용
605
XML 암호화 데이터?
아니오
예
606
복호화 요청
아니오
예
607
복호화 파라미터 설정
608
복호화
609
보안 정보 전송
종료

【도 7】